

Test Project

Module A2

Implementing Security Configurations

Cyber Security

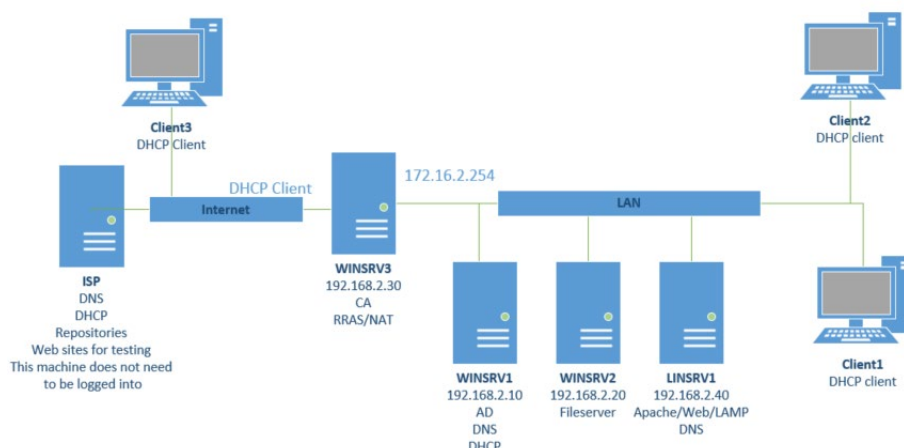
Contents

Contents	2
Introduction to Test Project	3
Introduction.....	4
<i>Physical Topology</i>	<i>4</i>
<i>Logical Topology.....</i>	<i>4</i>
<i>Table 1. VM Finished Configuration Summary.....</i>	<i>5</i>
Description of project and tasks.....	6
<i>ISP</i>	<i>6</i>
<i>Firewall configuration</i>	<i>6</i>
<i>Table 1. Firewall settings.....</i>	<i>7</i>
<i>PKI.....</i>	<i>8</i>
<i>WINSRV1.....</i>	<i>8</i>
<i>LINSRV1</i>	<i>9</i>
<i>LAN clients.....</i>	<i>9</i>
<i>WinClient3.....</i>	<i>9</i>
Instructions to the Competitor.....	9
<i>Table 2. GPO Policy Recommendations</i>	<i>10</i>

Introduction to Test Project

Our friends over at skill 39 have built a network for a client, and everything works as expected, but things are not as secure as they need to be. The network when first examined was as follows:

Pre-project topology:



Following a security assessment, a number of changes needed to be made in order to make the network more secure: installation and configuration of a proper firewall, hardening of the domain and the Linux machines, management of a Public Key Infrastructure, and segmenting the network into different subnets, amongst other things, all need to be accomplished. In order to do the assessment and simplify the network, the File Services requirements were moved to WinSRV1.

You will be given a list of tasks to implement to work towards hardening the network and the systems on it, you and your partner will have to best decide how to spend your time to get all the configurations done. You will be assessed on the completeness of these tasks based on both a configuration and functional standpoint, so remember to test your configurations as you go.

Use the following login credentials to log onto the ESXi server for the afternoon portion of the activity:

IP Address: **192.168.1.1**

User: **pmuser**

Password: **Paul Bocuse**

Login credentials for the competitor Laptops are as follows:

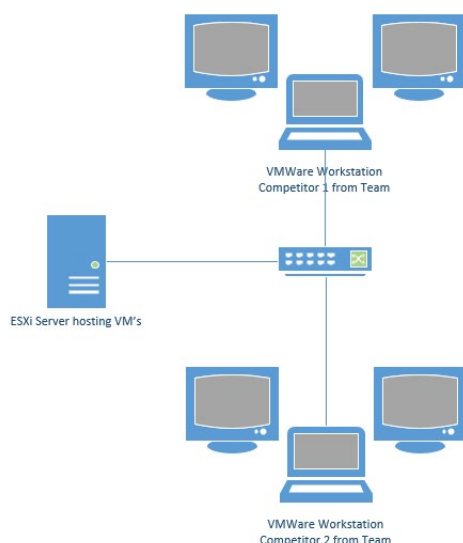
User: **Competitor0**

Password: **CharterDressing**

Introduction

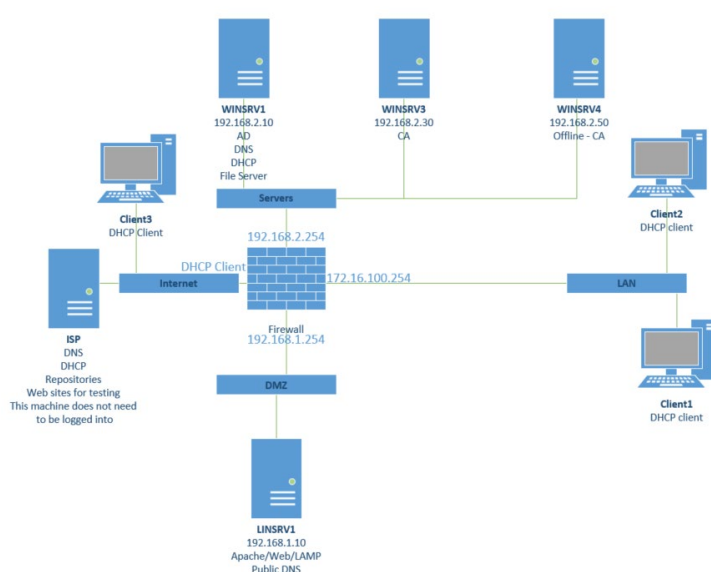
Physical Topology

The physical topology of this project is as follows: competitors from each team will use VMWare Workstation to access VM's hosted on a local ESXi server. All teams will have the same configuration and VM's, but only have access to their own VM's. As per the following diagram:



Logical Topology

The logical topology of the VM's provided on the ESXi server is as follows with the following Network configuration:



The VM's should all be preset with the correct IP addresses, subnet masks, and gateways, but it is the Competitor's responsibility to verify or identify any errors or discrepancy between the VM's provided and this documentation, and to correct them if necessary.

Table 1. VM Finished Configuration Summary

VIRTUAL MACHINE	VLAN	IP ADDRESS	NOTES	CREDENTIALS
ISP	Internet		Offers DNS and website access to locally connected machines – serves as the “fake Internet” for connection testing. Competitors should not need access to this machine for any reason.	N/A
Client1 and Client2	LAN	DHCP Client	Internal access and testing	Two machines have been provided to allow testing of different settings in the event competitors need to be testing different things at the same time. Access via any existing Domain Users with a password of P@ssw0rd
Client3	Internet	DHCP Client	For testing VPN and Websites in DMZ – can be moved to LAN if required but should be left as DHCP client on Internet VLAN	Can use a domain account or local administrator or competitor account – both with a password of P@ssw0rd
WINSRV1	SERVERS	192.168.2.10/24	DC for AD, DNS and DHCP for Internal Clients and servers	All Users in AD have a password of “ P@ssw0rd ” – do not modify the passwords unless required by the project
WINSRV3	SERVERS	192.168.2.30/24	Issuing CA	CA servers have been installed, but you will need to finish the installation as per the project
WINSRV4	SERVERS	192.168.2.50/24	Off line Root CA	

VIRTUAL MACHINE	VLAN	IP ADDRESS	NOTES	CREDENTIALS
LINSRV1	DMZ	192.168.1.10/24	Public facing DNS entries Website hosting	root/P@ssw0rd competitor/P@ssw0rd Access to be setup as per the project All required software is pre-installed but may need to be configured
FIREWALL	Connected to all VLANs	192.168.2.254 (Server) DHCP Client (Internet) 192.168.1.254 (DMZ) 172.16.100.254 (LAN)	All traffic except that specified in the project is blocked.	Admin/pfsense

Description of project and tasks

Configure and test the settings for the following systems:

ISP

This machine is simulating the Internet. It is running a DHCP server which will service the WAN interface on the router and Client3, the external client. This machine will operate as the “upstream” DNS server and hosts two websites to test the Firewall configuration from Internal clients. The two websites are:

<https://www.letour.fr>

<https://www.moulinrouge.com>

The purpose of these websites is for testing firewall configuration and have been created intentionally with a self-signed certificate.

Competitors will not need to logon to this machine, and do not have logon credentials for it. It needs simply to be on to provide DHCP/DNS/web services for testing.

Firewall configuration

The firewall is installed in its base configuration, with IP and interfaces connected to the proper subnets, and IP's assigned no other configurations have been done. Default logon to PFSense is admin/pfsense.

It is important to functionally test firewall configuration from the machines on various networks to verify functionality and not rely strictly on configurations.

- Set admin user password to be **“P@ssw0rd”**
- Setup DHCP for LAN clients on PFSense – WinSRV1 should be the DNS Server

Block all traffic except as listed:

Table 1. Firewall settings

SOURCE NETWORK	DESTINATION NETWORK	PORTS/SERVICES ALLOWED	NOTES
LAN	Internet	Outbound and return traffic to WAN allowed	
LAN	DMZ	Ssh, http, https, DNS allowed to LINSRV1	
LAN	Servers	For AD TCP/UDP - 53, 88, 135, 137-139, 389, 443 445, 464, 636, 3268-3269 For PKI: TCP – 9389	
WAN	Inbound WAN traffic to website and DNS in DMZ allowed	http, https, DNS	
Servers	As necessary for services		
DMZ	Servers/AD	TCP/UDP - 53, 88, 135, 137-138, 389, 445, 464, 636, 3268-3269	

In addition to traffic restrictions, implement the following on the firewall as well

- OpenVPN
 - Set up a VPN connection using OpenVPN where the client queries AD and uses a certificate produced by WinSRV3 as the CA cert. Packages have been pre-downloaded.
 - Members of the VPN Users group would be able to connect from WinClient3 to OpenVPN – can use a self signed certificate if you cannot get CA signed certificate.
- Snort
 - Install SNORT as IDS – should log all traffic going out to Internet. Package has been pre-downloaded
 - Attempts to access **www.moulinrouge.com** should be logged in Snort.
 - modify this custom rule in snort as appropriate and apply it to the WAN interface:

drop tcp any any <> a.b.c.d/24 and (flags: FPU; msg: "Possible XMAS scan"; sid: 100001)

- This rule can be tested by initiating a port scan in nmap from Client3

Internet access:

- Set rules that will allow your Internal clients to access the **www.letour.fr** site on the Internet, but will block access to **www.moulinrouge.com**.

PKI

2 Tier PKI

WinSRV4 will be offline RootCA, this is already configured and powered off. You should not need to turn this on unless you wish to troubleshoot an issue, it is included for completeness and in industry would be completely powered off and removed from network access.

WinSRV3 will be the issuing CA.

This machine is already configured as the subordinate (issuing) CA for the domain. Complete the following tasks:

- Create a new Group Policy Object called "**certenroll**" so that computers on the domain will automatically receive a certificate from the issuing CA through application of the GPO. These GPO's should be set to autoenroll.
- When an internal client browses to either of the following websites, it should not be prompted with a certificate error on connection, since the root-ca should be recognized as a trusted CA via policy.
 - Through autoenrollment, WinSRV3 should receive a certificate for the Web server in the IIS installation.
 - Also install a certificate onto the LINSRV1 for the Website there.

WINSRV1

Note – Wireshark has been installed on this machine for troubleshooting purposes.

- Create a password policy that requires all domain user's passwords to be 8 characters in length, must be changed monthly
- Create a fine-grained password policy that requires members of the executive group to have a 10 character long password
- Create a login banner/title that says "**WorldSkills Lyon**"
- Create a login banner/text that says "**authorized access only**"
-
- Create a GPO called "**control**" that will restrict access to the control panel – which is only applicable to accounting users
- Create a GPO called "**registry**" that will prevent access to registry editing tools – only applicable to users in Paris
- **Import chrome policy** – in the documents folder of the domain administrative account is the googleChromeEnterpriseBundle64. Extract the contents of this file, create a GPO called "google" and use the admx files to create a policy that will force all users to use the company website at <http://w3.lumiere.com> as the default home page.
- The client would like you to recommend three other GPO's which should be created to help better secure the domain. Fill in table 2 in the appendix describing what the effect is of the GPO's you have chosen, and why you chose these GPO settings over other possible GPO settings. This document should be saved on the desktop of the competitor computer and be sure when finishing that experts are able to find/collect the file.
- Create a share on WinSRV1 following best practices at the local path C:\shares\pictures shared as "pictures" that will allow the Read access to the customer service group, Modify (RW) for members of the Graphics group, FC for IT, no access for anyone else.
- In the C:\shares\picture folder, you will find a picture called "paris.jpg", set auditing on this file so it is logged when read by a member of any group.

LINSRV1

- Join LinSRV1 to Lumiere.com domain.
- All other domain machines should be able to resolve the name to IP address of LINSRV1.
- access allowed for domain users C1 and C2 via ssh

If you can't domain join LinSRV1 and use the C1 and C2 domain user accounts, create matching local C1 and C2 accounts so any further assessments can be completed. Allow the C1 and C2 (either domain or local) users to have administrative rights through sudo.

- Both C1 and C2 users should be able to use all root level administrative commands through the use of the sudo commands.
- Other users which connect will not have elevated sudo privileges.
- Local firewall setup
 - Firewall should be running
 - Services for required operation permanently added to the firewall to be operational after a reboot
- Ssh configurations
 - Have ssh listen on port #2022
 - Root not allowed to connect via ssh
 - Only C1 and C2 users can connect via ssh
- Set the passwords for any locally created Linux users to match that in the domain
 - 10 characters in length
 - Password changed every month
 - Minimum password length of 25 days
 - Warn a user their password will expire after 25 days
 - Password must have one lower case, upper one case, and one numerical digit

httpd is installed on the server is set up to host the http:// website contained in /var/www/lum. This website should be available to both domain users in the LAN network, and from remote clients on the Internet.

- Set this site up to use https:// preferably using a certificate signed by WinSRV3, but if you cannot get this to work, use a self-signed certificate.
- enable SELinux but make certain the httpd service is still fully operational.

LAN clients

Note – wireshark and putty have been installed on these machines for troubleshooting purposes.

- Use these machines to functionally verify requirements specified in other sections

WinClient3

Note - Nmap is installed if you wish to initiate a port scan on the firewall.

- Remote access to network via VPN
- Test website and DNS access for DMZ

Instructions to the Competitor

All existing user accounts have a password of **P@ssw0rd** including the root and administrator accounts.

We know that this is a weak password to use and have done this for ease of use and assessment at the competition and should not be considered a vulnerability. Please do not change or reset the passwords unless directed by the project as experts will be unable to login and assess your configurations.

All server VM's have statically configured IP addresses. You are responsible verifying if these are set correctly in the case that a setting on a virtual machine is different than this document.

This document will be provided digitally on the competitor workstation, combine the answer documents to a single file for submission. When you signal to experts that you are done it will be collected.

Table 2. GPO Policy Recommendations

NAME OF POLICY TO BE INCLUDED IN GPO RECOMMENDED	PATH TO SETTING IN POLICY	EFFECTS OF APPLYING THIS GPO	WHY DID YOU SELECT THIS GPO OVER OTHER POSSIBLE CHOICES?